

עמוד 1 מתוך 17

WS – GOV.IL תקן ל-GATEWAY הממשלתי נספח ג' – תעודות דיגיטאליות -CERTIFICATES

גרסה 2.3

מסמך זה כולל מידע השייך לממשל זמין, רשות התקשוב הממשלתי. כל חשיפה, שימוש או העתקה של מסמך זה או חלקים ממנו – ללא קבלת אישור בכתב ממנהל מערך סייבר ואבטחת מידע בממשל זמין – אסורה בהחלט. מסמך זה מיועד לעובדי ממשל זמין ולקוחותיו



עמוד 2 מתוך 17

מעקב גרסאות

תיאור השינויים	עודכן על ידי	תאריך	מס"ד
זו גירסה 2.0 מספטמבר 2015 - בתבנית חדשה	אופיר יהב	11.10.2015	2.1
של ממשל זמין.			
הוספת הערה לחלק הכללי.	אופיר יהב	12.10.2015	2.2
שינוי לוגו והוספת נתוני גרסת המסמך	יוני ארוך	29.11.2015	2.3

נתוני גרסת המסמך

חתימה	תאריך	שם מלא	תפקיד	גורם
(חתימה)	11.10.2015	אופיר יהב	РМО	נערכה ע"י
(חתימה)	11.10.2015	אלעד פז	מוביל טכנולוגיות במערך סייבר ואבט"מ	נבדקה ע"י
(חתימה)	11.10.2015	אברהם זרוק	מנהל מערך סייבר ואבט"מ	אושרה ע"י



עמוד 3 מתוך 17

<u>תוכן עניינים</u>

4	כללי	.1
4	מסמכים ישימים	.2
4	התהליך	.3
6	סרטיפיקטים	.4
6	Machine Certificate סדר פעולות להפקת	4.1
13	בדיקת הרשאות על תעודה	.5



1. כללי

web services מבוסס על התקן העולמי ws-security המפרט כיצד ניתן לאבטח web services עקן העולמי יעקן ". ע"י הזדהות ואימות המסרים העוברים בין השרת ללקוח.

תקן ws-security מאפשר מספר מנגנוני הזדהות, אך תקן ws.gov.il מאפשר הזדהות ע"י חתימה דיגיטלית בעזרת X.509 v3 certificate בלבד.

במהותו תקן ws.gov.il מחייב כל צד (שרת ולקוח) לחתום דיגיטלית כל מסר יוצא, ולוודא (verify) כל מסר נכנס. בנוסף, לכל צד יש רשימה של ישויות המורשים לפנות אליו, כך שבתהליך הווידוי, בנוסף לווידוא החתימה נבדק כי הפונה רשאי לפנות לצד זה.

מסמך זה מתייחס למערכות הפעלה שנמצאות במחזור החיים של Microsoft.

מסמך זה מפרט את הפעולות השונות לביצוע התהליכים הבאים:

- 1. התקנת תעודות ה-CA.
- .Machine Certificate התקנת תעודת מכונה.

ממשל זמין שם לעצמו למטרה לאפשר ללקוחותיו, וכלל המשתמשים, שירותים מאובטחים ורציפים. מסמך זה כולל, בין היתר, הנחיות אבטחת מידע ודרישות טכניות הנגזרות מהן. רק הקפדה על הנחיות ודרישות אלו תיצור מעטפת הגנה מיטבית על השירותים ותשמור על רציפותם של השירותים.

2. מסמכים ישימים

.WS-gov.il מסמך זה הינו חלק מתקן WS-gov.il.

3.התהליך

יש לעבוד לפי השלבים ולשנות (במידת הצורך) את ההגדרות לפי המסכים שיוצגו.



עמוד 5 מתוך 17



4. סרטיפיקטים

על מחשב שמשמש כשרת החושף Web-Services דרך רשת ה-gateway הממשלתית יש CA להתקין machine-certificate בעל יכולת להצפין ולחתום על מידע, שנחתם על ידי משל זמין - תמוז.

נהלי ממשל זמין לא מאפשרים לבצע export ל-private keys של הסרטיפיקטים המונפקים על ידי ממשל זמין ולכן יש לבצע מתוך השרת עצמו בקשה להנפקת סרטיפיקט, לשלוח את הבקשה לצוות PKI בממשל זמין ולהתקין את התעודה שתתקבל. בנוסף על מנת שהסרטיפיקט יזוהה לצוות DKI במאושר יש להתקין את ה-public certificates של ממשל זמין. התעודות מותקנות כאשר מריצים את הסקריפט לבקשה ליצירת תעודה.

4.1 סדר פעולות להפקת Machine Certificate

- . כאמור לעיל, אין תמיכה במערכות הפעלה שאינן נתמכות במיקרוסופט. <u>https://support.microsoft.com/he-il/lifecycle</u> ניתן לעיין בקישור המצורף
- 2. יש לגלוש לכתובת <u>http://147.237.72.65/public/util/G2/Request</u> עלגוש לכתובת G2_Computer_Config_2008.zip עבור מערכת ההפעלה: win 2008 ומעלה.
 - .3. יש לשים את הקובץ על השרת/מחשב שעבורו רוצים לייצר תעודה.
 - 4. יש לעשות Unzip לקובץ.
- 5. יש לעבור ל- Start/AllPrograms/Accessories/CommandPrompt הלחוץ על הכפור הימני ולבחור באפשרות של Run as administrator.



מוד 7 מתוך 17 איז איז איז איז איז איז איז איז איז איז	Pictures
Connect to a Connect to a Conne	Open Run as administrator Open file location EditPlus 3 Scan with OfficeScan Client Add to archive Add to "cmd.rar" Pin to Taskbar Pin to Start Menu Backup
 Sync Center Windows Ex Windows M WordPad Ease of Acce System Tool Tablet PC Windows Pc 	Restore previous versions Send to Cut Copy Delete Rename
Back Search programs and Machine (Constraint)	Properties <i>files</i> Lingvo 6.0 Computer signe

- 6. בשורת הפקודה עברו לתיקייה G2_Computer_Config_2008.
 - .cert_request.bat יש להריץ את הקובץ.
 - .8. לחצו על OK אם קופץ חלון.



עמוד 8 מתוך 17



- 9. את הקובץ שנוצר בשם ComputerName.txt יש לשלוח לצוות SOA לחתימה. לנוחיותכם, רצ"ב כתובת האימייל SOAteam@gov.il
- 01. את הקובץ שנשלח אליך בחזרה מצוות SOA בשם ComputerName.cer.txt לשנות ל- ComputerName.cer.
 - a) יש לשים את הקובץ ComputerName.cer בתיקיה (a
- (4 עיש להריץ cert_accept.bat יש להריץ מdministrator-) יש להריץ (b
 - :יש לבחור באופציה OK כאשר יעלה חלון עם ההודעה הבאה (c

Certifical	te Request Processor 🛛 🗙
8	Cannot find object or property. 0x80092004 (-2146885628)
	OK

- ניתן לעשות זאת MMC (Microsoft management console) 11. יש להריץ את באמצעות ה Run.
- File -> Add/Remove Snap-In... א לבחור בתפריט של החלון שנפתח את...12



עמוד 9 מתוך 17 Console1 - [Console Root] File Action View Favorites Window Help New Ctrl+N Ctrl+O Open... Save Ctrl+S Save As... Add/Remove Snap-in... Ctrl+M Options... 1 C:\Users\...\Console1.msc 2 compmgmt.msc 3 eventvwr.msc 4 gpedit.msc Exit

Certificates->ComputerAccount->LocalComputer 13. יש לבחור ב 13





עמוד 10 מתוך 17

certificate ולבחור ב Certificates->Personal->Certificates ולבחור ב 14. יש לעבור ל

Console1 - [Console Root\Certifie	cates (Local Computer)\Pers	onal\Certificates]
File Action View Favorite	s Window Help	_ & ×
Console Root	Issued To	Actions
Certificates (Local Compute Personal	Igor-W7	Certificates
Certificates	篇Igor-W7 篇IGOR-W7.tehila.gov.il	More Actions
Trusted Root Certificatic		Igor-W7 🔺
 Enterprise Trust Intermediate Certificatic Trusted Publishers Untrusted Certificates Third-Party Root Certific Trusted People Other People Remote Desktop Certificate Enrollment R Smart Card Trusted Roo Trusted Devices 		More Actions
	•	<u> </u>
	_	



עמוד 11 מתוך 17

.private key	ולוודא שיש י	certificate	את ה	לפתוח	יש.	15
--------------	--------------	-------------	------	-------	-----	----

6	Certificate Inform	ation
Thi	• certificate is intende • Proves your identity to • Ensures the identity of	ed for the following purpose(s): o a remote computer f a remote computer
	Issued to: Igor-W7	
	Issued by: TAMUZ - D	Devices CA
_	Valid from 8/22/2010	to 8/21/2012
9	You have a private key	that corresponds to this certificate.
		Issuer <u>S</u> tateme
earn n	ore about <u>certificates</u>	



עמוד 12 מתוך 17



5. בדיקת הרשאות על תעודה

- 1. עבור מערכת הפעלה 2008 ומעלה:
- ניתן לעשות זאת MMC (Microsoft management console) יש להריץ את (a באמצעות ה Run.
- File -> Add/Remove Snap-In... יש לבחור בתפריט של החלון שנפתח את (b

File	Action View Favorites New Open Save	Window He Ctrl+N Ctrl+O	elp	
	New Open Save	Ctrl+N Ctrl+O	-	
	Open Save	Ctrl+O		
	Save			
	ourc .	Ctrl+S		
	Save As			
	Add/Remove Snap-in	Ctrl+M		
	Options			
	1 C:\Users\\Console1.msc			
2 compmgmt.msc				
	3 eventvwr.msc			
	4 gpedit.msc			
	Exit			
		Add/Remove Snap-in Options 1 C:\Users\\Console1.msc 2 compmgmt.msc 3 eventvwr.msc 4 gpedit.msc Exit	Add/Remove Snap-in Ctrl+M Options 1 C:\Users\\Console1.msc 2 compmgmt.msc 3 eventvwr.msc 4 gpedit.msc Exit	



עמוד 14 מתוך 17



Certificates->ComputerAccount->LocalComputer ביש לבחור ב





- Manage יש ללחוץ על הכפתור הימני בעכבר ולבחור ב-All Tasks ואז e. Private Keys...
- של ה- identity. יש לבדוק האם למשתמש שמפעיל את השירות (ה- identity של ה-על התעודה. אם אין, יש להוסיף Full Control את ההרשאות. את ההרשאות.



17 -	מתוך	16	עמוד

.ADD	סיף אותו ע"י לחיצה על כפתור Permissions for sapssl private 🕌	א קיים, יש להוכ keys פ	אם המשתמש לא שלים	.g
	Security <u>G</u> roup or user names: <u>SYSTEM</u> Shuli Tryster Administrators (shuli-T\Admin	nistrators)		
	Permissions for SYSTEM	A <u>d</u> d Allow	<u>R</u> emove Deny	
	Read Special permissions	V		
	For special permissions or advance click Advanced.	ced settings,	Ad <u>v</u> anced	
	ОК	Cancel		

ואז ללחוץ על Full Control אז ללחוץ על .h

		.0
Select User, Computer, Service Account, or Group		? ×
Select this object type:		
User, Group, or Built-in security principal		Object Types
From this location:		
tehila.gov.il		Locations
Enter the object name to select (<u>examples</u>):		
[IIS-User]		Check Names
Advanced	ОК	Cancel



עמוד 17 מתוך 17